ABSTRACT:

A method of generating a linear transformation matrix A for use in a symmetric-key cipher includes generating a binary [n,k,d] error-correcting code, where k < n < 2k, and d is the minimum distance of the binary error-correcting code. The code is represented by a generator matrix $G \in \mathbf{Z}_2^{k\times n}$ in a standard form $G = (I_k \,||\, B)$, with $B \in \mathbf{Z}_2^{k\times(n-k)}$. The matrix B is extended with 2k-n columns such that a resulting matrix C is non-singular. The linear transformation matrix A is derived from matrix C. Preferably, the error correcting code is based on an XBCH code.

FIG. 5.